United States Patent [19]

Shear

[11] **Patent Number: 5,050,213**

[45] **Date of Patent: * Sep. 17, 1991**

[54] **DATABASE USAGE METERING AND PROTECTION SYSTEM AND METHOD**

[75] Inventor: **Victor H. Shear, Bethesda, Md.**

[73] Assignee: **Electronic Publishing Resources, Inc., Bethesda, Md.**

[*] Notice: The portion of the term of this patent subsequent to May 2, 2006 has been disclaimed.

[21] Appl. No.: **562,996**

[22] Filed: **Aug. 6, 1990**

Related U.S. Application Data

[60] Continuation of Ser. No. 310,938, Feb. 16, 1989, Pat. No. 4,977,594, which is a division of Ser. No. 918,109, Oct. 14, 1986, Pat. No. 4,827,508.

[51] **Int. Cl.**[5] **H04L 9/32; G06F 13/14**

[52] **U.S. Cl.** **380/25**; 380/4; 380/50

[58] **Field of Search** 380/314 5, 23, 25, 22, 380/49, 50, 16; 364/200, 900

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,609,697	9/1971	Blevins	364/200
3,956,615	5/1976	Anderson et al.	380/25 X
4,120,030	10/1978	Johnstone	380/4
4,168,396	9/1979	Best	380/4
4,200,913	4/1980	Kuhar et al.	364/900
4,232,193	11/1980	Gerard	380/36
4,236,217	11/1980	Kennedy	364/483
4,253,157	2/1981	Kirschner et al.	364/900
4,305,131	12/1981	Best	364/521
4,306,289	12/1981	Lumley	380/4
4,319,079	3/1982	Best	380/4
4,361,877	11/1982	Dyer et al.	364/900
4,375,579	3/1983	Davida et al.	380/25 X
4,433,207	2/1984	Best	380/4
4,434,464	2/1984	Suzuki et al.	364/200
4,446,519	5/1984	Thomas	364/200
4,454,594	6/1984	Heffron et al.	364/900
4,458,315	7/1984	Uchenick	380/4
4,462,076	7/1984	Smith	364/200
4,462,078	7/1984	Ross	364/200
4,471,163	9/1984	Donald et al.	380/4
4,494,156	1/1985	Kadison et al.	360/48
4,513,174	4/1985	Herman	380/4
4,528,588	7/1985	Lofberg	358/349
4,553,252	11/1985	Egendorf	377/15
4,562,306	12/1985	Chou et al.	380/4
4,562,495	12/1985	Bond et al.	360/78.04
4,577,289	3/1986	Comerford et al.	364/900

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

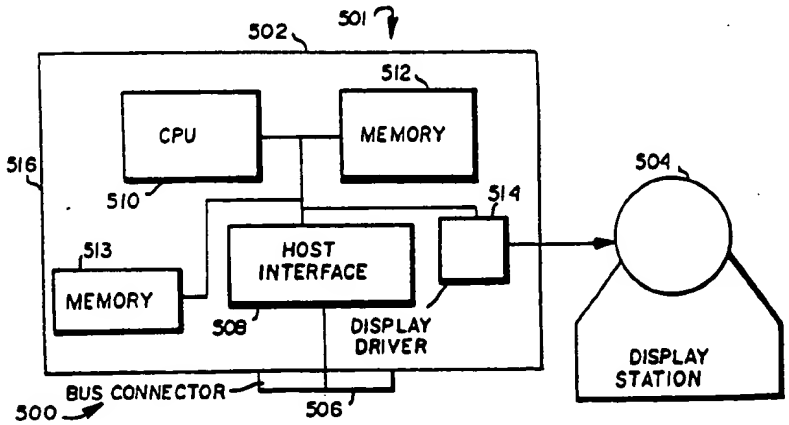
85/03584 8/1985 PCT Int'l Appl. .

Primary Examiner—Bernarr E. Gregory
Attorney, Agent, or Firm—Nixon & Vanderhye

[57] **ABSTRACT**

A "return on investment" digital database usage metering, billing, and security system includes a hardware device which is plugged into a computer system bus (or into a serial or other functionally adequate connector) and a software program system resident in the hardware device. One or more data bases are encrypted and stored on a non-volatile mass storage device (e.g., an optical disk). A tamper-proof decrypting device and associated controller decrypts selected portions of the stored database and measures the quantity of information which is decrypted. This measured quantity information is communicated to a remote centralized billing facility and used to charge the user a fee based on database usage. A system may include a "self-destruct" feature which disables system operation upon occurence of a predetermined event unless the user implements an "antidote"—instructions for implementing the antidote being given to him by the database owner only if the user pays his bill. Absolute database security and billing based on database usage are thus provided in a system environment wherein all database access tasks are performed at the user's site. Moreover, a free market competitive environment is supported because literary property royalities can be calculated based on actual use.

25 Claims, 5 Drawing Sheets



U.S. PATENT DOCUMENTS

4,584,641	4/1986	Guglielmino	364/200
4,588,991	5/1986	Atalla	380/4
4,589,064	5/1986	Chiba et al.	364/200
4,593,353	6/1986	Pickholtz	364/200
4,593,376	6/1986	Volk	364/900
4,595,950	6/1986	Lofberg	380/5
4,597,058	6/1986	Izumi et al.	364/900
4,634,807	1/1987	Chorley et al.	380/4
4,644,493	2/1987	Chandra et al.	364/900
4,646,234	2/1987	Tolman et al.	364/200
4,652,990	3/1987	Pailen et al.	364/200
4,658,093	4/1987	Hellman	380/25
4,670,857	6/1987	Rackman	380/4
4,680,731	7/1987	Izumi et al.	364/900
4,683,553	7/1987	Mollier	380/4
4,685,056	8/1987	Barnsdale et al.	364/200
4,688,169	8/1987	Joshi	364/200
4,691,350	9/1987	Kleijne et al.	380/3
4,696,034	9/1987	Wiedemer	380/16
4,701,846	10/1987	Ikeda et al.	364/200
4,713,753	12/1987	Boebert et al.	364/200
4,740,890	4/1988	William	364/200
4,747,139	5/1988	Taaffe	380/44
4,757,533	7/1988	Allen et al.	380/25
4,791,565	12/1988	Dunham et al.	364/200
4,827,508	5/1989	Shear	380/4

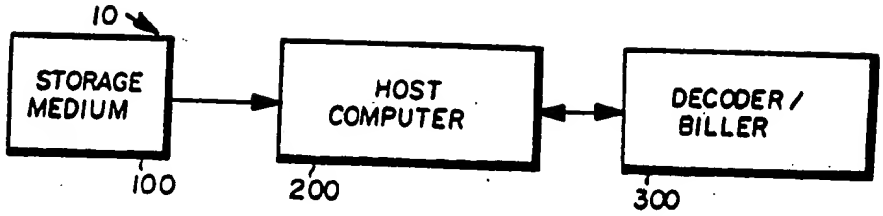
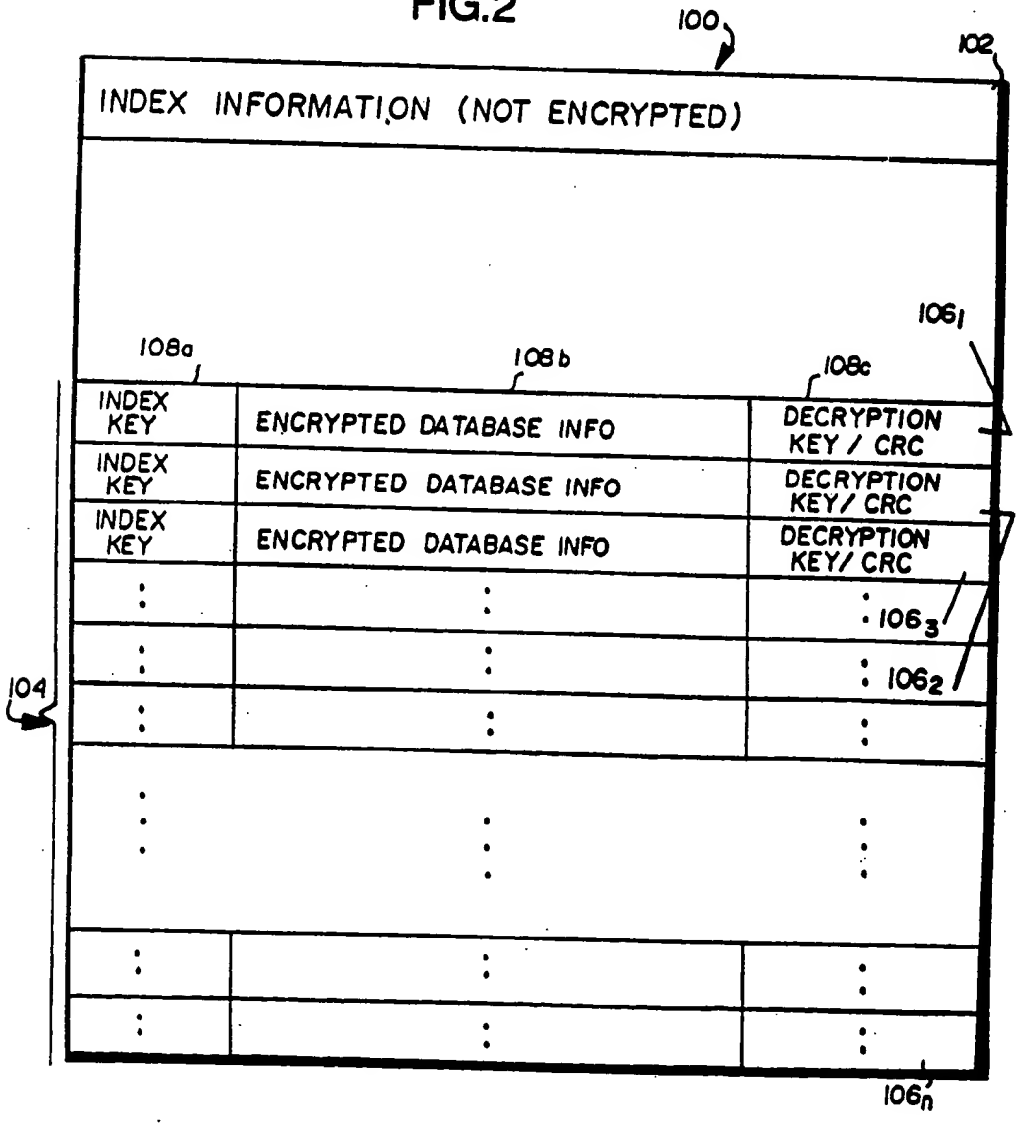

10
STORAGE MEDIUM
100
HOST COMPUTER
200
DECODER / BILLER
300

FIG.1

FIG.2


100
102
INDEX INFORMATION (NOT ENCRYPTED)
106₁
108a
108b
108c
INDEX KEY
ENCRYPTED DATABASE INFO
DECRYPTION KEY / CRC
INDEX KEY
ENCRYPTED DATABASE INFO
DECRYPTION KEY/ CRC
INDEX KEY
ENCRYPTED DATABASE INFO
DECRYPTION KEY/ CRC
106₃
106₂
104
106n

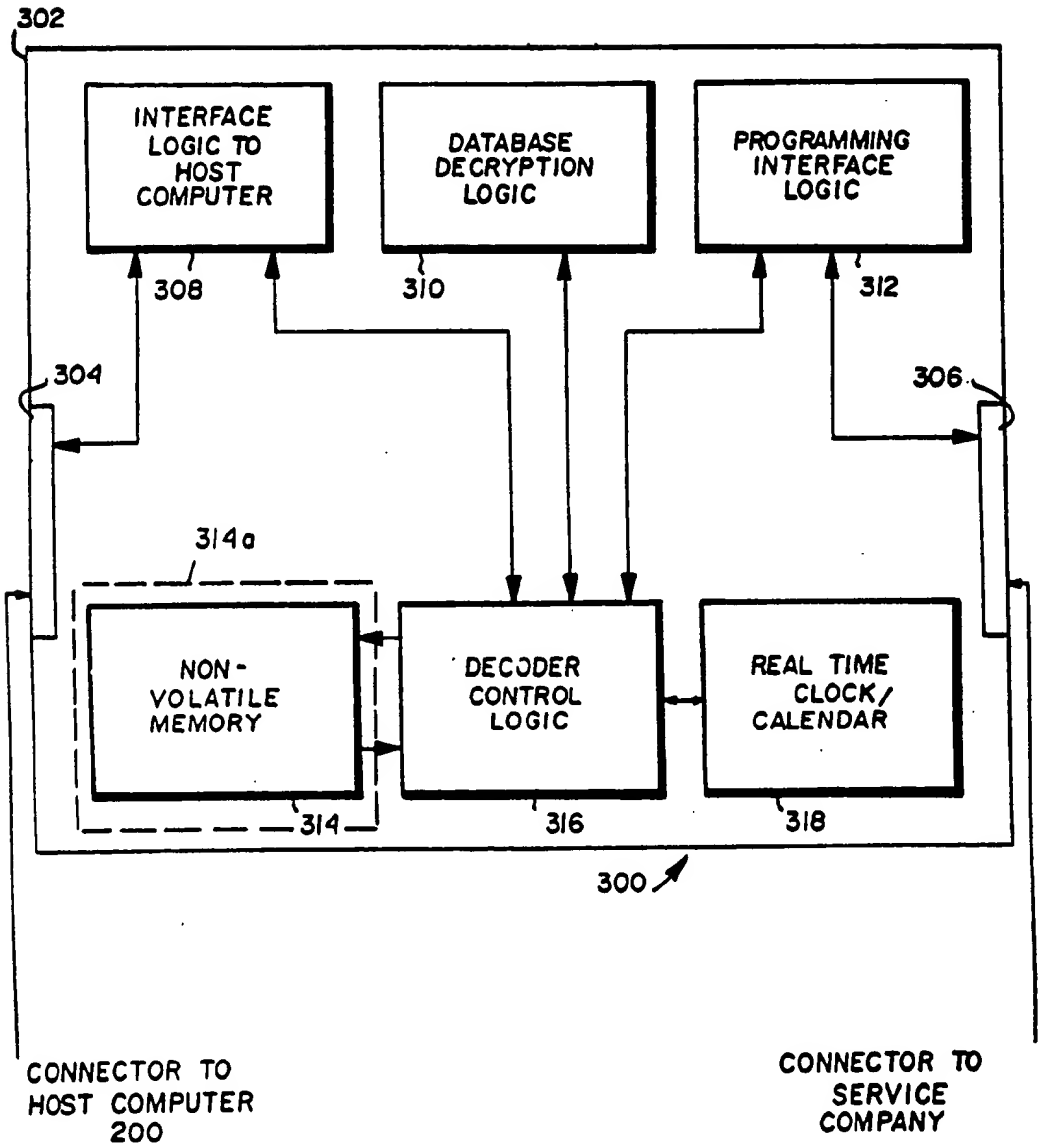

302
INTERFACE LOGIC TO HOST COMPUTER
DATABASE DECRYPTION LOGIC
PROGRAMMING INTERFACE LOGIC
308
310
312
304
306
314a
NON-VOLATILE MEMORY
DECODER CONTROL LOGIC
REAL TIME CLOCK/ CALENDAR
314
316
318
300
CONNECTOR TO HOST COMPUTER 200
CONNECTOR TO SERVICE COMPANY

FIG.3

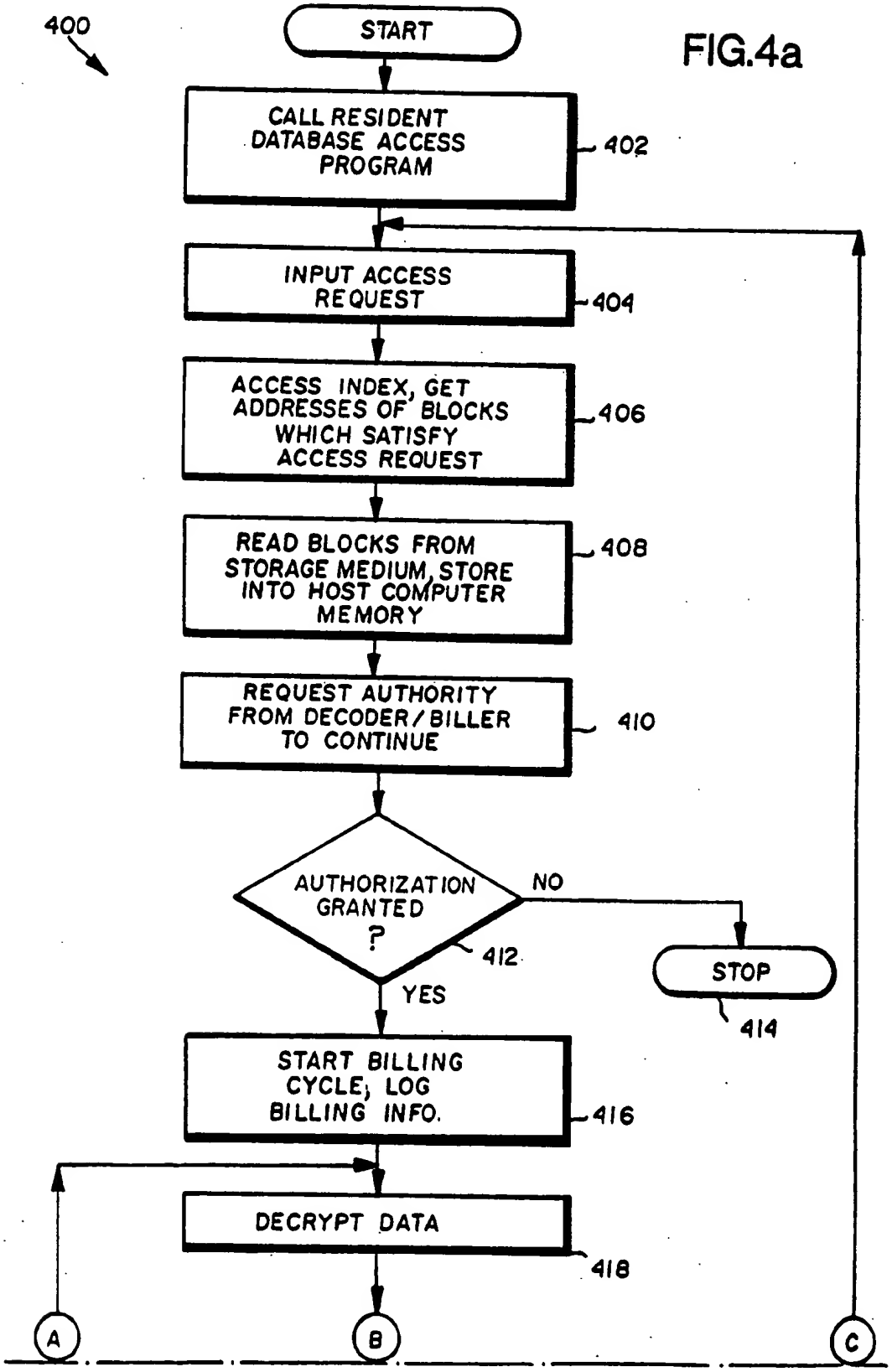

400
START
CALL RESIDENT DATABASE ACCESS PROGRAM
402
INPUT ACCESS REQUEST
404
ACCESS INDEX, GET ADDRESSES OF BLOCKS WHICH SATISFY ACCESS REQUEST
406
READ BLOCKS FROM STORAGE MEDIUM, STORE INTO HOST COMPUTER MEMORY
408
REQUEST AUTHORITY FROM DECODER/BILLER TO CONTINUE
410
AUTHORIZATION GRANTED ?
412
NO
STOP
414
YES
START BILLING CYCLE; LOG BILLING INFO.
416
DECRYPT DATA
418
A
B
C

FIG.4a

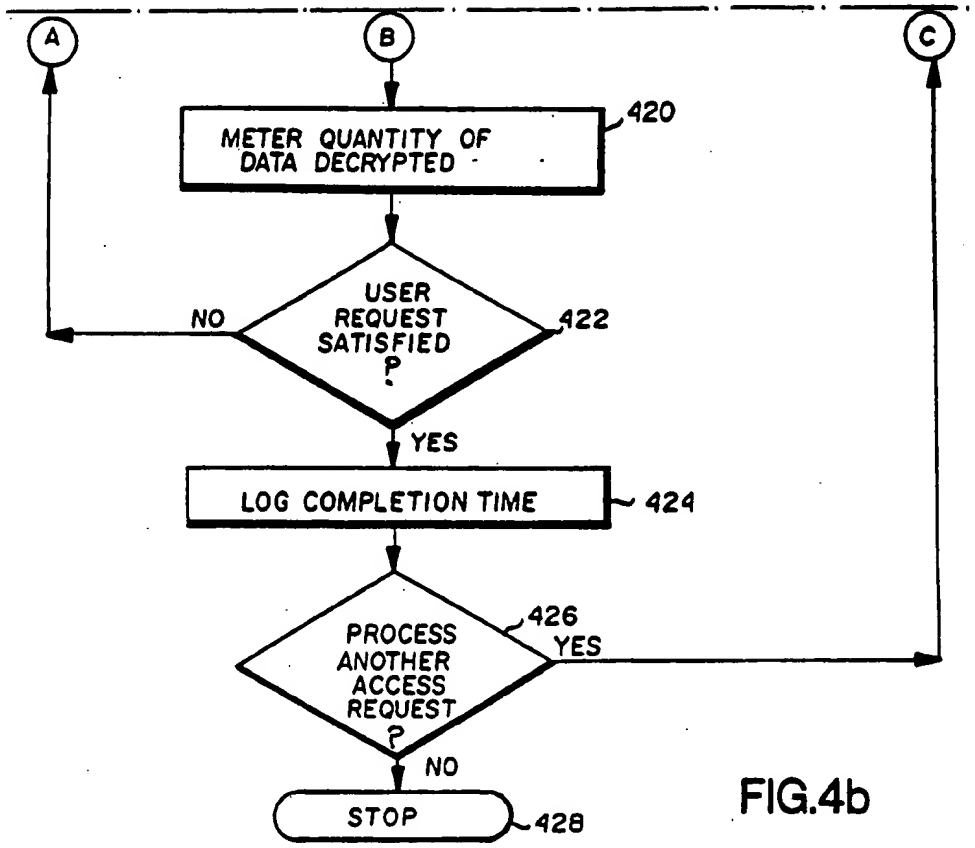

A
B
C
METER QUANTITY OF DATA DECRYPTED
420
USER REQUEST SATISFIED ?
NO
422
YES
LOG COMPLETION TIME
424
PROCESS ANOTHER ACCESS REQUEST ?
426
YES
NO
STOP
428

FIG.4b

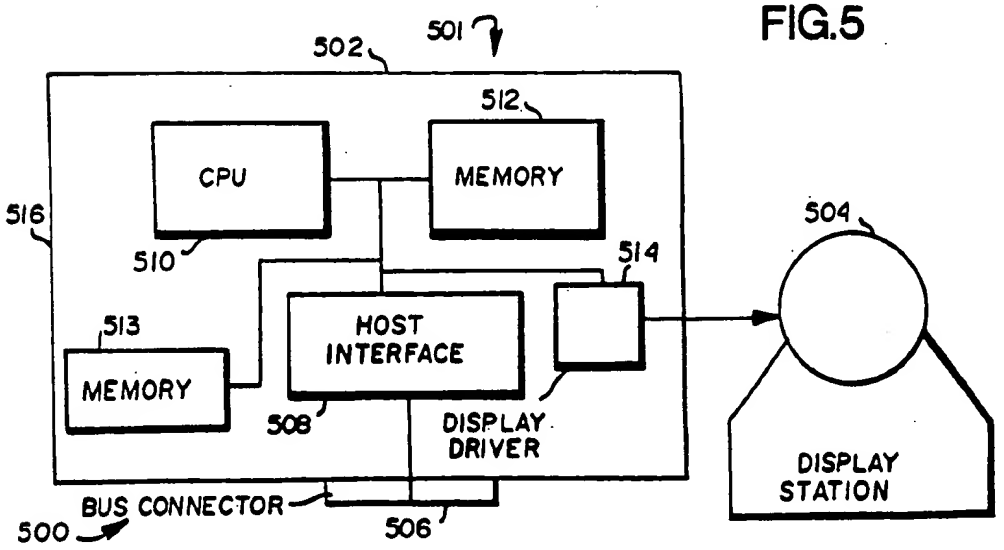

502
501
512
CPU
MEMORY
516
504
510
514
513
HOST INTERFACE
MEMORY
508
DISPLAY DRIVER
DISPLAY STATION
BUS CONNECTOR
500
506

FIG.5

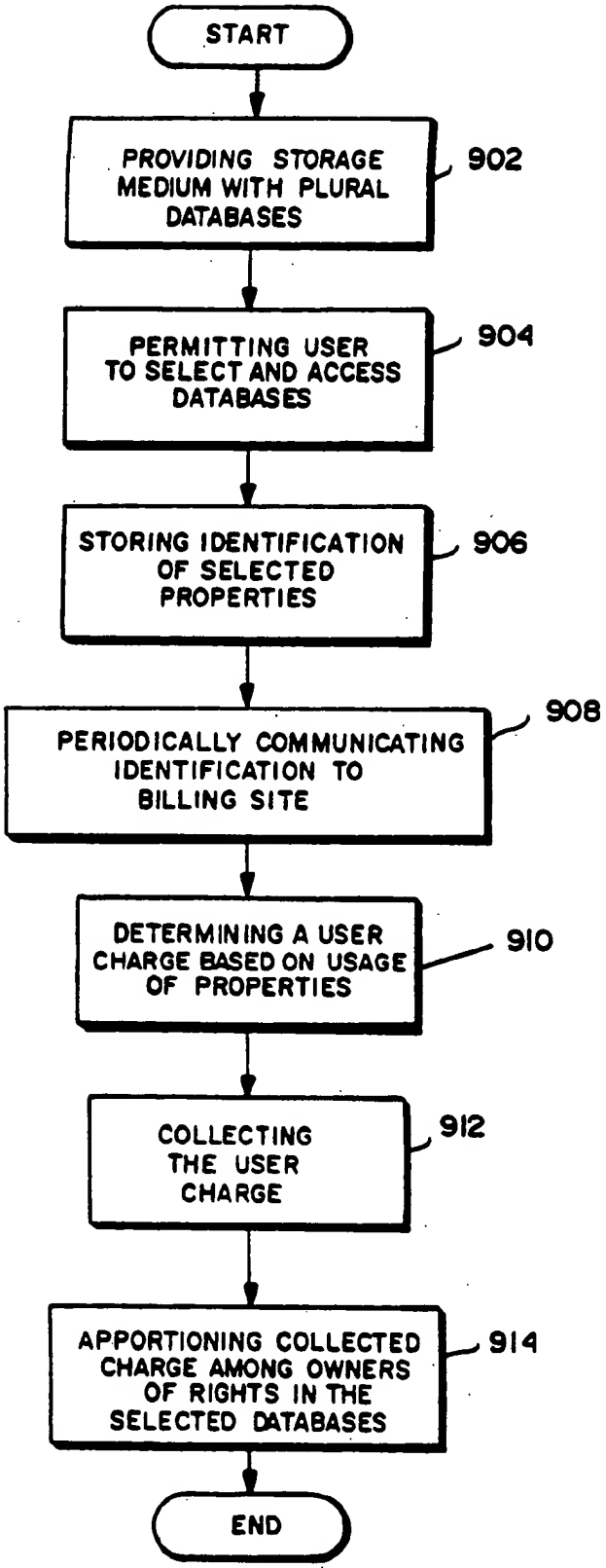

START
PROVIDING STORAGE MEDIUM WITH PLURAL DATABASES
902
PERMITTING USER TO SELECT AND ACCESS DATABASES
904
STORING IDENTIFICATION OF SELECTED PROPERTIES
906
PERIODICALLY COMMUNICATING IDENTIFICATION TO BILLING SITE
908
DETERMINING A USER CHARGE BASED ON USAGE OF PROPERTIES
910
COLLECTING THE USER CHARGE
912
APPORTIONING COLLECTED CHARGE AMONG OWNERS OF RIGHTS IN THE SELECTED DATABASES
914
END

FIG.6

DATABASE USAGE METERING AND PROTECTION SYSTEM AND METHOD

This is a continuation of application Ser. No. 07/310,938 filed Feb. 16, 1989, now U.S. Pat. No. 4,977,594, which is a divisional of application Ser. No. 06/918,109, filed Oct. 14, 1986, which is now U.S. Pat. No. 4,827,508.

The present invention relates to regulating usage of a computer database. More particularly, the invention relates to techniques for preventing unauthorized use of an electronic digital information database and for measuring the utilization of the database by authorized users.

Information conveyed in electronic form is rapidly becoming the most valuable of commodities. Electronic digital databases now exist for a variety of different applications and fields of endeavor, and many businesses presently rely heavily on their ability to access those databases.

The value of being able to instantaneously, electronically access important, accurate information cannot be overestimated. Many of our daily activities depend on our ability to obtain pertinent information in a timely fashion. While printed publications and electronic mass media together fulfill most of the average person's informational needs and most often are the only source for full-text reference information, just about any effort to access information can benefit from the vast information handling capabilities of the computer. In today's fast-paced world, we quickly come to insist on and rely upon the most thorough and up-to-the-minute information available —often made possible only by electronic data processing and informational management technology. On-line, public databases, now a two billion dollar a year industry, are a case in point.

As the "information explosion" continues its course, more and more people will become dependent on electronically-stored information and people will continue to be willing to pay premium prices (when necessary) for access to and use of such information because of its usefulness and value to them. Currently, the principal resource for large, electronic information data bases are on-line (public) data base services such as Dialog Information Services, Mead Data Central, Dow Jones Information Services, Source, Compuserve, and many others. Most on-line data bases are abstract and/or bibliographic in content, and many are used primarily to access the document locations of specified information, rather than for the recall of the original document full-text.

Historically, personal computers have been used primarily for word-processing, modeling, and, to a lesser extent, the structured data base management of records. Technology that enables the user of, for example, a personal computer to search for, locate, and retrieve topically related full-text information from vast full-text data bases would be extremely useful and valuable.

The only viable way to make some kinds of information (e.g., information which must be constantly updated) available is to maintain centralized databases and permit users to access the centralized databases through telephone lines or other communication means. Until very recently, this method has been the most cost-effective way to offer access to electronic databases. Access to a centralized database can be controlled relatively easily, and users can be charged for using a centralized database in accordance with parameters which are relatively easy to measure (i.e., the amount of time the user is connected to the database computer, the number and type of tasks the user requests, etc.). Moreover, because the database never leaves the central computer (each user is typically given access to only small portions of the database at a time), there is no danger of someone making unauthorized copies of the database.

However, centralized databases have important disadvantages. For example, it takes a relatively long time to manipulate information in a centralized database due to the relatively slow data transmission rates of standard communications channels and because the centralized database computer typically shares its resources among hundred or thousands of users at once. This can be a serious drawback if the user wishes to access a large volume of information or wishes to perform particularly complex data manipulation tasks. Also, it may take a long time during periods of peak database usage before communication can be successfully established with a centralized database computer, decreasing the utilization of the database and causing some users to become frustrated. Further disadvantages include the expense of establishing long-distance communications paths (e.g., WATS telephone line maintenance charges, long-distance direct-dial telephone charges, satellite channel costs, etc.) between distant user terminals and the central database computer, and the reliability problems associated with such communications paths. Moreover, the centralized computer facility needed to handle the access requests of many distant users simultaneously is extremely expensive to purchase and maintain.

With the advent of cheaper computer hardware and new, high density information storage devices (such as the optical disk and the bubble memory), it has become practical to give users their own copies of large and complex databases and permit users to access and manipulate the databases using their own computer equipment. Optical disks are capable of storing vast amounts of information at relatively low cost, are small enough to be sent through the mails, and can provide data at extremely rapid rates. Bubble memory devices provide some similar capabilities.

CD and related digital disk devices can currently store up to 225,000 pages of full-text information per removable diskette and can inexpensively maintain in excess of 1,800,000 pages of text simultaneously on-line. These technologies are ideal for personal computer information base libraries. CD drives use removable compact disks (essentially identical to an audio compact disk) the very low cost and enormous storage capacity has been predicted to result in an installed base of as large as one million drives to 10 million drives (including non-CD but related optical storage technology) by the end of 1990. Owners of "CD-ROM" and related drives will create an enormous demand for both lexical software and electronically published information base products. Mitsubishi Research Institute of Japan, for example, estimates that between 8,000 and 12,000 different CD-ROM publication titles will be on the market by the end of 1990.

Hence, it is now possible to store some databases on transportable, high-density information storage devices, and simply mail each user his own copy of the databases. The user can in this way be given exclusive access, via his own computer system, to local, on-site databases. Rapid access time is provided because access to the databases is exclusive rather than shared, and

because data can be read from the database storage device by local high-speed I/O devices and transmitted over local high-speed I/O channels or networks. The stored databases can be updated periodically if necessary by sending the user storage devices containing a new version of (or new portions of) the databases.

It is very expensive to build a database. One way to recover the costs of constructing and maintaining a database ("Return On Investment", or ROI) is to charge a flat subscription or access fee to each user subscribing to use the database. If this is the only billing method used, however, infrequent users of the database may be discouraged from subscribing, because they would be asked to pay the same cost a frequent user pays. Thus, many database owners charge subscribers a nominal subscription fee, and then periodically (e.g., monthly) charge users a fee calculated in accordance with the amount the user has used the database.

While it is easy to measure the amount someone uses a centralized database (e.g., simply time each access session length and store the time information with user identification information), there is no convenient way to measure the usage of a database residing on a user's own computer, or to convey such usage information to the owner of the database. Techniques are known for automatically, electronically measuring consumption of a commodity such as electricity, water or gas, storing the measurements in a memory device, and periodically downloading the stored measurements over a telephone line to a central billing computer. Unfortunately, these known techniques are not readily adaptable to database usage metering, and moreover, are neither secure enough nor provide the security against database piracy that most database owners demand.

The prevention of unauthorized database usage becomes a huge problem whenever a stored database leaves the possession and control of the database owner. Computer program manufacturers lose millions of dollars each year to "pirates" who make unauthorized copies of software and distribute those copies for profit. Complex databases are often even more expensive to produce than programs, so that potential contributors of data base properties, as well as database owners themselves, may be extremely hesitant to permit electronic copies of their properties or databases to leave their control unless they can be absolutely sure no unauthorized copies will be made. The copyright laws and contractual licensing agreements may deter, but will not prevent, unauthorized use and copying of database.

SUMMARY OF THE INVENTION

The present invention provides a database access system and method at a user site which permits authorized users to access and use the database and absolutely prevents unauthorized database use and copying. The present invention also provides a facility for measuring usage of the on-site database for the purpose of billing the user according to the amount he has used the database, and for periodically conveying the measured usage information to the database owner (or his agent)—while preventing the user from tampering with the measured usage information.

The invention solves fundamental media based electronic publishing issues including:

Security of the information base. The present invention provides a code/decode Interlock System which includes both software and a tamper proof hardware module that prevents unauthorized and/or unmetered use of a protected information base. The present invention also supports a multi-level coded security access system limiting access to various portions of a data base only to those individuals possessing the proper security code(s); and

Ascertaining the degree of usage of the information base. The present invention stores, in one of several alternative forms of non-volatile

memory, the dates and times that any files (or documents, sections, properties, etc.) are accessed and also records the amount of information read from each file into memory by the user.

With the present invention, a CD-ROM disk, for example, might contain all issues of 10 separate publications (technical, medical, business, etc.) going back for five years. Each publisher would be able to set the price for the use of its publication or publications and each publisher could then receive a "copyright royalty" return-on-investment based on the actual customer usage of the publishers' products. Therefore, publishers contributing more important, popular or costly to develop lexical information base properties could earn revenues commensurate with the market demands and pricing strategies for their products.

The present invention eliminates the necessity of determining how much of the net revenue of a CD information base product each contributing publisher should receive (currently an issue of considerable concern to publishers). The present invention also ensures the data security of information bases—a critical, frequently voiced, and previously unanswered problem causing considerable publisher anxiety. It would be quite difficult (requiring a high level of specialized expertise and costly high-powered computers) to "break" the hardware/software data security system provided by the present invention and copy material without being charged an appropriate fee.

Publishers can license their products at an exceptionally low initial cost to customers (i.e. for a $25.00 initial fee instead of a $1,000.00 or more annual fee). Low initial licensing fees would result from the usage auditing capability of the present invention and would allow new clients to experiment with the product at little or no risk. Similarly, customers who anticipate a low level usage of a given information base product may find the lower costs of a usage based fee schedule a practical and affordable justification to acquire a product that would otherwise not be purchased.

In sum, the present invention will:

1. Significantly accelerate market penetration of electronically published products due to substantially lower initial license costs;

2. Greatly enhance the ultimate market penetration of CD published products by making CD publications affordable to a much large body of customers; and

3. Produce higher ultimate revenues per published disk from those customers who would otherwise have purchased a costlier version of the database product.

The security protection provided by the present invention will give publishers significant advantages in securing exclusive contracts for important publishing information base properties, since the invention provides the information base property contributors with:

1. Vastly superior copy protection security;

2. Ultimately greater revenue;

3. Publisher specific control over pricing; and

4. A return-on-investment commensurate with the market demand for their information base property.

In accordance with one important feature of the present invention, a storage medium stores the database in encrypted form, and also stores index information which correlates portions of the encrypted database with index keys. The index information may itself be encrypted if desired. A host digital signal processor operatively connected to the storage medium is preprogramed so as to generate a database access request, read the index information from the storage medium, identify (in accordance with the index information) the portions of the encrypted database which satisfy the access request, and read the identified encrypted database portions from the storage medium.

A secure decoder control logic device coupled to the host processor receives the encrypted database portions read by the host processor, decrypts portions of the encrypted database read by the host processor to produce corresponding decrypted information, and transmits the decrypted information back to the host processor. The decoder control logic device also measures the quantity of usage of and/or other parameters pertaining to the information decrypted by the decrypting device, and stores these measurements in a non-volatile (and in many cases tamperproof) memory device. The invention thus provides a detailed record of database usage—including a breakdown of usage of each file or "property" stored on a local storage medium. Additional decryption of database information can be prevented or disabled if more than a certain percentage of a database (or more than a specified contiguous portion of a database) has been copied by the user as an additional safeguard preventing unauthorized copying.

The system may further include means for preventing tampering with the memory device and/or the decoder control logic means.

In accordance with another important feature of the present invention, database usage information is stored at a user's site and is periodically communicated to a central billing facility. For example, the non-volatile memory device storing data indicating database usage may be housed in a replaceable module. Periodically, the user disconnects the module from his computer system and sends it to a centralized billing facility. At the centralized billing facility, the contents of the memory device are read and used to bill the user according to his database usage.

In accordance with yet another important aspect of the present invention, communications is periodically established between the user's site and a central facility for the purpose of telecommunicating database usage information stored at the user's site to the central facility.

In accordance with yet another important feature of the invention, the user is automatically prevented from decrypting the encrypted database after a predetermined event occurs (e.g., "expiration" of a memory module, or excessive database usage indicating copying attempts) unless the user has implemented an "antidote" (e.g., input secret information into his computer system and/or install a replacement component).

Because the database is stored in encrypted form (and/or the database directory is encrypted or otherwise coded), the only way to obtain useful database information is to decrypt portions of it using the tamperproof decrypting means of the invention. Safeguards may thus be used to prevent unauthorized database decryption.

Thus, the present invention resolves several fundamental problems that would otherwise impede the rate of growth of the CD-ROM and CDI electronic publishing markets. For example, it is a costly process to create the core properties that may be incorporated into an information data base, and the structuring of the data base itself may, in some circumstances, be a costly effort. One way for data base preparers to recover the costs of constructing and maintaining a database is to charge a flat subscription or access fee to each user subscribing to use the database. If this is the only billing method used, however, infrequent users of the database may be discouraged from subscribing —because they would be asked to pay the same cost a frequent user pays. Furthermore, potential users may be hesitant to pay a significant one time or initial fee to acquire a technology or product with which they are unfamiliar.

With the present invention, a user will be able to pay (if so structured by the data base provider) according to his usage of the product and both the perceived risk, as well as—in lower usage environments—the high cost of the use of the technology, can be reduced or eliminated. Furthermore, since the present invention should accelerate the installed base and revenue growth rate for a given product, it may enable costs for even the high volume users to drop as well.

Moreover, database use can be measured simply by measuring the quantity of information which is decrypted. Other parameters relating to database usage (e.g., which databases and/or database subdivisions have been used; and the time, date and duration of use of each database and/or subdivision) may also be monitored and stored. The stored usage information can be periodically communicated to a centralized facility for billing the user in accordance with his database usage. Moreover, the user's on-site database access system can be designed to cease functioning unless the user installs a new component and/or inputs "secret" information—and the centralized facility can provide the user with such replacement components and/or secret information only when the user has paid his bill.

Because the invention provides a detailed record of which literary properties have been used and how much each property has been used, use payments paid by the user may be fairly apportioned to the property owners according to actual use of their respective properties. For example, if a user licenses a storage medium storing a library containing hundreds of different literary properties and then uses only two properties in the library, the owners of those two properties can be paid substantially all of the licensing fees charged to the user.

A free market system is thus maintained in an environment not otherwise susceptible to free market competition. Publishers and authors can be assured that they will receive incomes based on customer demand for their properties, and publishers can retain absolute control over pricing—despite the fact that the properties are being distributed on a storage medium along with hundreds of other properties. "Best sellers" can still be distinguished from unpopular works, and authors can be paid royalties based on consumer demand for their works.

This invention thus solves the fundamental CD and Optical publishing problem of how to provide end-users with disk libraries containing many different publications from different venders. Different properties from different publishers have differing significances in the today's marketplace. These products have prices which

each reflect vendor investment, product specific market demand, and other vendor product marketing considerations. The present invention allows each vendor to set a price for their product(s) carried on CD or other media publications. The invention has an interlock system that prevents access to the non-volatile storage media (such as a CD-ROM disk) unless the user has contracted for the use of the disk and has a hardware plug-in module incorporating software.

When a customer makes use of stored data, the invention monitors which files are accessed and how much information is requested by the user to be displayed. In one embodiment of the present invention, information that is being reviewed or browsed may be distinguished from information that is read into a host computer for the purpose of copying, modifying, or telecommunicating, with different cost rates being applied to the different activities (so that, for example, the cost of browsing can be much less than the cost of copying or printing). Depending on the specific application and the nature of the user contract, the user might be required to:

1. Telephone the publisher once every three months, establishing a modem link over which a request is transmitted to telecommunicate back to the publisher the meter usage data; or

2. Mail to the publisher once every three months a removable EPROM module that contains the metered usage data.

The present invention thus prevents copying or browsing of a protected information base without adequate compensation to the publisher and its information base property (data) suppliers. Each supplier of information to an information base product receives a return on investment that reflects both the market demand for his specific property and the pricing and other marketing strategies that the supplier deems appropriate for his product.

The present invention allows very large numbers of customers to acquire library disks at very low initial costs, since the customer's billing can be largely based on usage, not simply possession of the library disk. As a result, potential customers, regardless of size or financing, will be able to maintain very broad based libraries on-site. If a given group regularly uses only a fraction of the information base, the group's users can still search the entire data base whenever appropriate. This means that most user billing is concentrated on those reference resources that the users frequently use, but an entire, comprehensive reference library extending beyond the user's frequent requirements is immediately available for use. A publisher will be in a much better position to provide large scale reference information base libraries. In many applications, the breadth and comprehensiveness of these encyclopedic libraries will encourage much more frequent use and a much larger body of users.

The present invention thus answers both the needs of a potentially very large customer base for low cost initial access to comprehensive digital disk based reference libraries, while at the same time maintaining supplier publisher control over pricing and guaranteeing an appropriate return on investment based on the customers demand for their products.

The invention may be particularly attractive to the owners of the leading properties in a given vertical publishing market, since these owners are likely to be particularly sensitive to the issues of unauthorized access to and copying of their product, pricing of their product, and equitable return on the value of the contribution of their product to an information base library. These publishers are likely to greatly increase their revenues through participation in library publication and distribution in accordance with the present invention—and the presence of such publishers in the marketplace will make it economically necessary (and feasible) for other publishers who have second tier properties to contribute to the same information base product.

The present invention may also include an optional security system which allows an organization to prevent usage of all or a portion of an information base unless the user enters his security code. Multiple levels of security codes can be supported to allow restriction of an individual's access according to his security authorization level.

There is significant value in using the present invention with certain types of non full-text information bases. For example, an electronic, CD disk containing comprehensive telephone white pages, telephone yellow pages, and as additional options, individual specific additional information (including estimated income level, publications received, job type and position, social security number, and other information that is compatible and legally available from one or more of the various mailing list companies) might be used with the present invention.

As a result of the present invention, the telephone operating companies providing directory listings can be compensated on the usage of their data base, while the mail order companies can also receive a revenue stream based on both usefulness of their data bases usefulness to customers and the extent of customer usage of their information. The present invention provides, for the first time, a context in which firms such as telephone operating companies and other information property suppliers can safely and profitably supply information for desk-top electronic information base products.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features and advantages of the present invention will be better and more completely understood by referring to the following detailed description of preferred embodiments in conjunction with the appended sheets of drawings, of which:

FIG. **1** is a schematic block diagram of a presently preferred exemplary embodiment of a database usage metering and protection system in accordance with the present invention;

FIG. **2** is a schematic block diagram of the information stored in the storage medium block shown in FIG. **1**;

FIG. **3** is a more detailed schematic block diagram of the decoder/biller block shown in FIG. **1**;

FIGS. **4***a*–**4***b* are together a flow chart of the steps performed by the system shown in FIG. **1**; and

FIG. **5** is a schematic block diagram of a further presently preferred exemplary embodiment of a database usage metering and protection system in accordance with the present invention; and

FIG. **6** is a flowchart of an overall method for receiving a return on investment from databases at user sites.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

FIG. **1** is a schematic block diagram of a presently preferred exemplary embodiment of a database usage metering and protection system **10** in accordance with

the present invention. System **10** includes three main blocks: a storage medium block **100**, a host computer **200**, and a decoder/biller block **300**.

Predefined database(s) is (are) stored on storage medium **100** in encrypted form, and selective portions of the database(s) are read from the storage medium by host computer **200** (several different databases can be stored on the same medium, although the present invention in its simplest form uses only a single stored database which may contain multiple files, segments, "properties" or the like). Host computer **200** may be a computer dedicated to the task of accessing the stored databases, but need not be (for example, the host computer can be a general-purpose digital computer used to do a variety of different tasks).

Decoder/biller block **300** is connected to host computer **200**, and performs at least two important functions. Decoder/biller **300** decrypts portions of the stored databases on a user-need basis (e.g., after confirming the user has proper authority to access the databases) (see FIG. **6**, block **904**). Decoder/biller **300** also meters database usage, and generates usage information in a form which can periodically be conveyed to the owner of the databases (or his agent, e.g., a service company) (see FIG. **6**, blocks **906–908**). The usage information is typically used to calculate database access fee the user is to be charged (see FIG. **6**, blocks **910–914**).

Decoder/biller block **300** may take the form of a hardware unit (or card) electrically connected to and located in proximity to (or within) host computer **200**, or computer software executing on the host computer. Alternatively, decoder/billing block **300** might be located remotely to host computer **200** and communicate with the host computer via a data communications network or a telephone line.

Storage medium **100** is preferably some form of inexpensive mass digital information store (e.g., an optical disk, a bubble memory or a large hard disk or other fast transfer rate magnetic storage technology) prepared by the database owner and licensed to the user for use. CD-ROM, CDI, WORM, and other related optical/digital very large capacity storage modalities are now coming to the personal computer market and can be used for this purpose. These products are highly reliable, and very economically store hundred of megabytes up to multiple gigabytes of data.

For example, a CD-ROM diskette stores 550 megabytes of information on a single 12 centimeter laser diskette. CD-ROM technology now being released to the market will economically support up to eight parallel drives (4 gigabytes or 1,800,000 printed pages) and will access any desired sector in one second. In the next several years, technological advances should reduce access time to ½ second, and storage capacity will be doubled (450,000 pages per diskette and 3,600,000 pages on-line) if CD-ROM manufacturers decide to market double-sided disks and drives. CD-ROM, CDI, and WORM products will be increasingly affordable over the next 30 months, with CD-ROM prices estimated to drop from $800.00 to $400.00 or less per drive, including controller, and OEM and volume prices estimated to drop to as low as $175.00 per unit by 1990. With CD-ROM, WORM, and other optical/digital technologies, users can both purchase large scale information bases and also themselves easily build organization-specific information bases.

The database is preferably "preprocessed" and then stored onto medium **100**. The type of preprocessing performed depends upon the database and the application, but typically includes creating an encrypted rendition of the database and loading the encrypted rendition onto medium **100**. One or more of the many sophisticated conventional data encryption schemes which presently exist can be used for encrypting the database. Preprocessing preferably also includes generating an index to the database and storing the index together with the encrypted version of the database on the storage medium **100**. The index may or may not be encrypted.

The preprocessed database may be loaded onto storage medium **100** in a conventional fashion. For example, a "master" medium may be prepared, and then simply duplicated to yield a number of duplicate storage media **100**. Storage of the entire preprocessed database (or databases) may require several storage medium units (i.e., several optical disks), each unit storing a part of the database. The database can index one or more databases each containing one or more files, documents or "properties" (the term "properties" referring to a literary or other textual work protected by copyright).

FIG. **2** shows one exemplary scheme for storing database information on medium **100**. The information stored on medium **100** includes an index portion **102** and an encrypted database portion **104**. Database portion **104** includes a plurality of predefined quantities, or "blocks", **106** of digital data. Each block **106** includes three information "fields": an index key field **108***a;* an encrypted database information field **108***b;* and a decryption key/error-checking field **108***c*.

Index portion **102**, which may be encrypted, provides information used to translate a database access request into the addresses of one or more blocks **106**. The contents of index portion **102** depends on the type of database stored on medium **100** and the type of operations which are to be performed on the database. For example, if word or string searching is to be provided, index portion **102** may include a list of all of the words contained in the database and the blocks **106** in which the listed words appear. Index portion **102** may alternately (or also) include a "table of contents" of the database and a designation of the blocks **106** covering each entry in the table. Other ways to index a database are known, and the present invention is not limited to any particular indexing scheme.

Index key **108***a* of each block **106** stores data which can be referenced in accordance with information stored in index information portion **102**. Index key **108***a* may be explicit (e.g., a digital data word representing an indexing code or address) or implicit (e.g., physical "addresses" of storage medium **100** may themselves be used as indexing keys).

Encrypted database information fields **108***b* contains predetermined portions of the encrypted database. The size of these portions may be determined by the particular hardware and/or encryption techniques used, and is preferably (but need not be) fixed. If the nature of the database permits, logically-related information should be stored in the same blocks **106** (i.e., the database should be presorted and hierarchically organized) to reduce the number of accesses of storage medium **100** required to respond to a single user request. Techniques for organizing databases are known to those skilled in the art of information retrieval and database design and management.

02/28/2003, EAST Version: 1.03.0002

Decryption key/error-checking field 108c performs two functions in the preferred embodiment. First, it provides conventional error checking (e.g. CRC or parity) information useful for detecting information reading errors. Secondly, the field may provide information needed by sophisticated data decryption schemes to decrypt the information stored in associated field 108b. In many data decryption schemes, a decryption key word (which may itself be encrypted) carried with the encrypted data is used in conjunction with an additional data decryption key generated by the data decrypting device to decrypt the data. Field 108c may or may not be required depending upon the error checking and decryption schemes employed.

Host computer 200 contains resident software and hardware which provides an interface for all database transactions. Computer 200 includes one or more appropriate I/O handlers and associated hardware device drivers which permit the computer to read information from storage medium 100. Host computer 200 also includes appropriate data communications software and associated hardware which permits it to exchange data with decoder/biller block 300. The data communications pathway between host computer 200 and decoder/biller block 300 may be a shared data bus, a dedicated I/O channel, a shared data communications network, or the like.

When a user requests information from the database stored on storage medium 100, the computer program resident on computer 200 controls hardware of the computer to read the index information 102 stored on medium 100 in order to ascertain which database blocks 106 contain information specified by the user request. The computer program then controls host computer 200 to load one or more blocks 106 of the stored database information into the host computer memory. The host computer 200 then, under software control, strips off the contents of encrypted fields 108b from the blocks of information now resident in its memory (along with some or all of the contents of decryption key/CRC field 108c) and sends some or all of this information to the decoder/biller block 300 for processing.

Because the index portion 102 is not encrypted, host computer 200 can manipulate the index information without involving decoder/biller block 300. Although this is an important advantage in some applications (since the user is permitted to "browse" through the index "for free"), other applications may demand a level of security which is compromised by providing an unencrypted index. For example, unencrypted, very complete indexes might be used to reconstruct significant portions of the database itself. It may therefore be desirable to encrypt index portion 102 as well as database portion 104 to provide higher security.

If index portion 102 is encrypted, it must be decrypted before a user can make selections from it or otherwise use it to locate blocks 106. Decryption of index portion 102 should be performed in a secure environment (such as in decoder/biller block 300, or in a dedicated "browsing workstation" to be discussed in connection with FIG. 5). Alternatively, decoder/biller block 300 may temporarily provide host computer 200 with the decryption key information needed to decrypt index portion 102 (the index portion may be encrypted using an encryption technique which is different from the one used to encrypt database portion 104), and the host computer can decrypt sections of the index portion as needed by the user.

In one possible permutation of the invention, neither the database nor the index stored on medium 100 is "encrypted" using a formal encyrption algorithm, but instead, the manner in which the database and/or the index is stored on the storage medium is itself used to make information incoherent unless it is read from the medium using a predefined access algorithm.

For example, records of the database may be noncontiguously stored on medium in a pseudo-random order, so that sequential reading of records produces only incoherent information. An index stored on medium 100 contains the information needed to locate logically sequential database records. This index ("directory map") may also be in some way "scrambled" (for example, encrypted using formal encryption techniques, perhaps simply incomplete so that it must be supplemented with information and/or algorithms contained in decoder/biller block 300, or another scheme can be used to properly interpret the directory map, directory map interpretation being necessary to determine the locations on medium 100 of the components of a given database or other "property"). Different index scrambling schemes can be used for different copies of storage media 100 to prevent development of a "universal" de-scrambling device or algorithm.

Decoder/biller block 300 measures the amount and/or type of information sent to it for decryption and stores information indicating database usage over time from such measured amounts. Decoder/biller block 300 stores all necessary billing and usage information in a protected, non-volatile memory device (or in a protected, non-volatile storage facility within the host computer 200) for later retrieval and use in calculating database usage fees.

Because the database information read from medium 100 is useless unless it is first decrypted, and decoder/biller block 300 is the only portion of system 10 which is capable of decrypting the encrypted database information, the decoder/biller block can accurately meter the amount and nature of data accessed from the stored database e.g., by counting the number of blocks 106 which are encrypted, determining the group of logically related information ("property") stored on medium 100 which is logically associated with the data being decrypted, and/or determining other convenient parameters indicating the quantity and/or identity of data which is decrypted}. Decoder/biller block 300 decrypts the information sent to it, and returns the decrypted information to host computer 200 for display, storage, printing, telecommunications, or the like (or otherwise makes the decrypted information available to the user).

FIG. 3 is a more detailed schematic diagram of the decoder/biller block 300 shown in FIG. 1. Block 300 includes the following: a tamper-proof mechanism 302; a data connector 304 for connection to the host computer 200; a data connector 306 for connection to an off-site service company; host computer interface logic 308; database decryption logic 310; interface logic 312; a non-volatile memory 314; decoder control logic 316; and a real-time clock/calendar 318.

Tamper-proof mechanism 302 prevents unauthorized persons from electronically or mechanically tampering with decoder/biller block 300, and preferably includes both mechanical and electronic safeguards. For example, the physical enclosure which encapsulates the components of block 300 should prevent unauthorized individuals from accessing the enclosed components. The

components can be epoxied or potted if desired, and/or the enclosure can be provided with a mechanical seal which clearly evidences any tampering.

Another safeguard against tampering can be provided by implementing one of more of functional blocks 308–318 in the form of a custom integrated circuit. Such custom integrated circuits are not easily reproducible by an unauthorized person, nor could functional equivalents be designed ("black-boxed") so long as the techniques used to encrypt and decrypt the database are sophisticated. This level of data encryption sophistication is well within present technology.

Connector 304 and interface logic 308 communicate data between decoder/biller block 300 and host computer 200. Interface logic 308 includes conventional electronics which interface host computer 200 with decoder control logic 316. Interface logic 308 is electronically connected to physical electronic connector 304, which in turn is connected to a mating connector of host computer 200.

The exact configuration of interface logic 308 and connector 304 depends upon the nature of host computer 200 and sort of data communications pathway desired. For example, in one exemplary arrangement, connector 304 comprises a host computer bus connector (connected to the main bus of host computer 200 and addressed directly by the host computer processor) and interface logic 308 comprises a bus interface. Of course, connector 304 could comprise a standard RS-232 port connector and interface logic 308 could comprise conventional port interface logic—or the interface logic could comprise a communications controller (e.g., a data communications network controller or a modem) and the connector 304 could be a standard communications connector (if decoder/biller block 300 were located remotely from host computer 200).

Other communications connectors and/or ports might be used for connector 304, the specific arrangement used being chosen based on the application, convenient performance and/or cost. Other possible arrangements, including placing the decoder/biller block 300 into the same housing containing the drive which accesses medium 100, or connected to (or actually connected as part of) cabling connecting the drive for medium 100 to host computer 200, can be used.

Decoder control logic 316 preferably includes a conventional microprocessor pre-programmed with a predetermined control computer program, but might be implemented in other ways (e.g., as a discrete digital logic sequential state machine). Decoder control logic 316 controls all of the functions of decoder/biller block 300 in the preferred embodiment. Decoder control logic 316 also monitors database usage, produces digital data indicating the amount of such usage, and stores this data in non-volatile memory 314 for later retrieval (e.g., by a service company or the database owner).

Real time clock/calendar 318 permits database usage metering to indicate the time and date of each usage and the duration of usage, thus providing an important audit tool for both customers and the service company. In addition, this real-time clock/calendar 318 can be preprogrammed to allow the user to access certain databases only at pre-programmed times (e.g., by limiting access for given user security access codes).

Interface logic 312 and connector 306 may be used to communicate data with an off-site facility, such as the centralized computer of the database owner or a service company which handles periodic database usage billing. In one exemplary embodiment, connector 306 includes a standard telephone connector and interface logic 312 includes a standard modem. If desired, connectors 304 and 306 may comprise the same connector, and interface logic 308 and interface logic 312 may comprise the same components.

Database decryption logic 310 takes input digital data signals provided to it by decoder control logic 316 (these signals representing encrypted digital data read by host computer 200 from storage medium 100 and passed to the decoder control logic via connector 304 and interface logic 308), decrypts these digital data signals using a predefined decryption algorithm, and outputs decrypted data signals to the decoder control logic for display, printing, and the like. One or several different predefined decryption algorithms can be stored in (or hardwired within) decryption logic 310, and additional decryption algorithms can be downloaded into the decoder/biller block 300 as needed or required via interface logic 312.

Many conventional methods of encrypting/decrypting data are known, spanning from simple lookup tables to complex mathematical algorithms. The method of data encryption/decryption used depends on the amount of extra computer processing overhead and data storage space that the application will allow. It is not uncommon for substantial overhead to be needed to handle encrypted data.

To install system 10, storage medium 100 (along with its associated drive/access device) is connected to host computer 200, and decoder/biller 300 is also connected to the host computer port and/or bus (by connecting connector 304 as described). A non-volatile memory 314 is provided which has been preloaded with the following information (or is loaded upon installation):

(a) databases key(s) and/or password(s);
(b) billing rates (optional—may be performed by the database owner at his own facility);
(c) expiration data and "antidote" information; and
(d) user identification(s)/security levels (if desired).

FIGS. 4(A)–4(B) are together a high-level flowchart of the routine 400 performed by system 10 to access a portion of the stored database.

To access database information, the user causes host computer 200 to execute software resident within it which permits the user to formulate a database access request (block 402). As discussed above, the nature of the access request depends on the nature of the database and the needs of the user. Most users require the ability to perform lexical database searches (i.e., searches for words, strings, and the like). However, other methods of accessing information are also possible. For example, if the database is a literary novel, the user's access request might be a chapter number and/or page number. Personal Library Software, Inc. of Bethesda, Md., offers advanced indexing software technology which allows a user to perform both keyword and topical searches (contrasting with other commercial products, which are limited to keyword searching techniques). Personal Library software can be used to great advantage with the present invention.

The user then inputs an access request (block 404) using a keyboard or other standard I/O device connected to host computer 200. In response to the user's access request, host computer 200 accesses index portion 102 stored on medium 100 and obtains from the index portion the addresses of (or index keys corresponding to) each block 106 of the encrypted database

which satisfies the user's access request (block 406) (index portion decryption is performed at this time if necessary). Host computer 200 then reads the appropriate block(s) 106 of the encrypted database from storage medium 100 and stores these blocks of information into its own internal random access memory (block 408).

System 10 may require the user to input identification and/or password information along with his access request (block 404). System 10 checks the authority of the user to access the database by transmitting the inputted ID/password information to decoder/biller block 300 for comparison with a list of authorized IDs/passwords stored in memory 314 (block 410). If decoder/-biller block decoder control logic 316 denies authorization to continue with database access (because the inputted user information is incorrect, because the access request cannot be performed at the current time/date. etc.) (block 412). the decoder/biller block refuses to decrypt any data sent to it (block 414)—and may cease communicating with the host computer 200, and/or simply ignore any encrypted information the host computer sends it. While encrypted database information is already present in the memory of host computer 200, this encrypted information is incoherent and cannot be used for any useful purpose.

On the other hand, if decoder control logic 316 of decoder/biller 300 grants authority to proceed (block 412), the decoder control logic begins a "billing cycle", and stores information logging the billing cycle into non-volatile memory 314 (block 416). The information stored in memory 314 may include: (a) the name of the database file being accessed; (b) the section of the database being accessed (name, "property designation", file name, or other identification information); (c) the identification of the user accessing the database; and (d) the date and time the database access begins.

The information stored in non-volatile memory 314 may thus be used to create an "audit trail" which tracks different users (or groups of users) and their database usages. Special use passwords may be required to access selected databases, and actual use of all databases may be verified later from the information stored in memory 314. Such stored information is extremely valuable not only to help detect unmonitored database use, but also to allow detailed bills to be generated and to help determine which users among multiple users are responsible for generating usage charges. Such a detailed audit trail can be used to allow publishers and users to determine the detailed activities of users. This information can be used by users to determine what they are being charged for. The audit trail information can also be used by publishers and property owners to conduct marketing surveys—providing more detailed information about user demographics and information use than is presently available.

In addition, it may be desirable to code storage medium 100 (or particular databases or files stored on the medium) with unique (e.g., randomly-generated) user passwords by embedding secret password information in the database information. Non-volatile memory 314 can store information which matches the code associated with the particular copy of the storage medium licensed to a particular user. This coded information can be encrypted, and coding schemes and/or coded information may be changed periodically. Different users can be assigned different codes to prevent users from exchanging or sharing storage media 100.

This additional security feature also impedes the use of unauthorized decoder units (e.g., clandestine units manufactured to be similar to block 300). Such unauthorized units would not be equipped with the correct coded information, and even if they were, would work for only one similarly coded storage medium (or for only one or a few databases stored on a particular storage medium). The coding of storage medium 100 with embedded, user-identifying codes would also help to identify how any unauthorized copies of the database information came into being, since the coded information would be embedded in the database information itself and would thus also be present in any copies made from an original. Users found in this manner to be involved in copyright infringement could be penalized appropriately under the civil and criminal penalties of the copyright law, as well as for breach of their contractual obligations.

Decoder control logic 316 also is enabled at this time to begin (a) decrypting information sent to it by host computer 200 and (b) sending the decrypted information back to the host computer (block 418). Decoder control logic 316 meters the quantity and/or other usage parameters of data which is decrypted, and stores this usage information into non-volatile memory 314 along with the other billing information (block 420) (the decoder control logic may store quantity information directly into the memory, or may first convert it to billing information taking into account, for example, the cost of using the database file being accessed). This process continues until the user's request has been satisfied (as tested for by block 422).

The user can be billed an annual fee for unlimited use of some databases or database properties, and billed only for actual use of other databases or database properties. In this way, the user can pay a flat fee for the databases, or specific database properties or "books", he uses most often, and yet have access on a "pay-as-you-go" basis to other databases which he might use occasionally but not enough to justify paying the cost for unlimited use. This billing method provides the user with database resources he might not otherwise be able to afford, and also stimulates use of databases which are not used often but are nevertheless extremely valuable at times.

The specific steps performed to decrypt data (block 418) depends on the particular data encryption/decryption scheme used. Host computer 200 transmits encrypted data in predetermined quantities (e.g., fixed-length blocks) to interface logic 308 via connector 304 in the preferred embodiment. Interface logic 308 communicates this encrypted data to decoder control logic 316, which communicates it to data encryption/decryption logic 310. Logic 310 translates the encrypted data into intelligible information using a predetermined conventional decryption algorithm, and communicates the decrypted data back to decoder control logic 316. Decoder control logic 316 then communicates the decrypted data to host computer 200 via interface logic 308 and connector 304.

The database access program resident in the host computer then controls the host computer to display and/or print the decrypted information. If desired, the program resident in the host computer 200 can prevent the user from doing anything other than displaying (and/or printing) the decrypted data. Alternatively, this program may permit the user to manipulate the decrypted text (e.g., store the data in a disk file or in the

memory of the host computer) to permit the user to browse through full-text data at his leisure and/or to use this data for word processing, telecommunicating, or the like.

Decoder control logic **316** meters database usage (block **420**) by, for example, measuring the amount of information which is decrypted (e.g., by counting the number of fixed-length blocks which are decrypted; determining the source documents the decrypted information is associated with; and measuring the time, date and/or duration of access of the decrypted information). Control logic **316** may also record other billing information, such as the length of the database file being opened. Control logic **316** may be arranged to recognize the names or other designations of subsections of the database being accessed, allowing for different billing rates depending on the type or supplier of the information (so that use of more expensive databases can be billed at higher rates).

It may be desirable to not bill users for simply searching through the database (or at least, not bill at the full rate), but to bill only or at a higher rate for data that is decrypted and displayed, printed or communicated. It is for this reason that the database index is not itself encrypted in one embodiment—so that the user can browse through the index "for free" (or at a lower charge). As mentioned previously, however, it may be desirable in some instances to provide additional security by encrypting the index as well as the database. If decoder/biller block **300** decrypts the index, it can meter index usage and store this usage information into non-volatile memory **314**—thus permitting the user to be billed for index browsing at comparatively low rates. A dedicated "browsing terminal" (to be discussed shortly) may be used in some applications to provide a secure environment in which browsing can occur and billed at a rate which may differ from that for database information usage (e.g., printing, telecommunicating, copying, etc).

After the user's access request has been satisfied (as tested for by block **422**). the decoder control logic stores, into non-volatile memory **314**, the time the user finishes accessing the database. (block **424**). The resident program then allows the user to input another access request (using the same or different database) (block **426**). If the user does input another access request, the steps of blocks **404–426** are performed again (with blocks **416**, **420** and **424** causing an additional billing log entry to be stored in memory **314**).

The information stored in memory **314** is periodically communicated to the service company and used to bill the user for database usage. In one exemplary embodiment, memory **314** is housed in a storage module **314***a* which is easily separable from system **10**. Periodically, the user disconnects memory module **314** from decoder/biller block **300**, mails the module to the service company, and installs an alternative replacement module (the "next" module) into system **10**. Decoder control logic **316** disables data decryption unless a module **314***a* is connected to it (and perhaps also when the control logic has determined the non-volatile storage area is nearly full).

In another embodiment, communications between decoder/biller block **300** and the service company is periodically established for the purpose of downloading the contents of memory **314** to the service company billing computer. If connector **306** and programming interface logic **312** comprise a conventional standard telephone connector and associated modem, such communications can be established over standard telephone lines. The information stored in memory **314** is transmitted over the telephone line to the service company computer, and the service company computer then transmits commands which control decoder control logic **316** to reset the memory. In addition, the service company can establish communications with decoder/biller block **300** to monitor use of the databases stored on medium **100** (and detect misuse and unauthorized use). The service company may also control decoder/biller block **300** remotely (e.g., to disable it from operating if customer fails to pay his bill).

System **10** may include an enabling/disabling mechanism which prevents a user from accessing the stored database information if he fails to pay his bill. For example, in the embodiment discussed above having a separable memory module **314***a*, the service company can refuse to mail the user a replacement module until all outstanding balances are paid. If the customer fails to pay his bill, he will eventually fill up the memory module he has installed, causing decoder control logic **316** to disable data decryption (or alternatively, the modules **314***a* can be electronically data-coded, and the decoder control logic can refuse to permit decryption to be performed when the module date code is determined to be prior to the current date generated by real time clock/calendar **318**).

Decoder control logic **316** can be disabled from operating if the real time clock ever ceases to operate (for example, the clock may be battery powered and the battery might go dead after a year or so if scheduled preventive maintenance is not performed). Once the real time clock is repaired, a communications link can be established between decoder/biller block **300** and the central facility. The central facility can then read the contents of non-volatile memory **314**. If no suspicious or unauthorized activities have occurred, the central facility can reset real time clock **318** or check a locally set real time clock to permit normal database decoding operations to resume.

Another arrangement can control decoder control logic **316** to periodically, automatically change authorized passwords—and the service company can refuse to tell the customer the new passwords until the customer has paid his bill.

Alternatively or in addition to the arrangements discussed above, system **10** may be provided with an automatic "self-destruct" mechanism which automatically "destroys" a critical part of the system (e.g., the information stored on medium **100**, or the password table stored in non-volatile memory **314**) at a preset real time deadline (timed by real time clock/calendar **318**) unless the customer implements an "antidote" (e.g., inputs a series of secret code words) prior to the deadline. The service company can provide antidote instructions only to customers who have paid their bills. This automatic "self-destruct" mechanism can also be activated whenever the customer exceeds a predetermined maximum (and/or minimum) usage limit (so as to prevent a customer from running up a huge bill, from attempting to decrypt and store substantial portions of the unencrypted database, or from continuing to use the database in the unlikely event that he has successfully prevented the logging of usage information). If additional protection against database piracy is desired, the automatic "self-destruct" mechanism can also be activated whenever the user attempts to access, in one session or

over a number of different sessions or within a given time frame, more than a certain percentage of a given database and/or more than a certain number of contiguous blocks of (or logically related records or other subdivisions of) the same database. A permanent record of the blocks (records or other subdivisions) which have been accessed may be retained in non-volatile memory **314** so that the user can be prevented from copying an excessive amount or selected database properties or segments over a period determined by the database owner.

It may also be desirable to enable the user to program parameters stored in non-volatile memory **314** which limits the user's own use of database information stored on medium **100**. The routine shown in FIGS. **4(A)–4(B)** can provide a user interface with decoder/biller block **300** which permits a user to optionally store, in a user-accessible file within memory **314**, information representing ceilings on database usage or cost of usage over a period of time (e.g., a maximum monthly duration or cost for database usage, limitations on the type of information which can be decrypted, etc.). Decoder/biller block **300** keeps a running total of the parameter(s) the user has specified, and ceases decrypting database information if the total exceeds the user-specified parameter value. This feature permits the user to budget his database use, and is especially valuable in a business environment—since it permits an organization to directly limit the cost of database access by employees to an amount selected by the organization.

Although the embodiment shown in FIG. **1** is particularly suited for installation at a customer site, some applications might necessitate that decoder/biller block **300** and storage medium **100** be operated remotely to the customer site and communicate information to the customer via a communications link (e.g., a standard telephone line). In this "direct connect decryption" mode of operation, data decryption is performed at a central facility of the service company. Since only a small portion of the database is decrypted at any one time, a telephone line provides sufficient bandwidth to transmit the decrypted data at rates suitable for display by the customer's computer.

Using the "direct connect" mode, there is no need for periodic exchange of service storage modules or for pre-scheduled periodic communications with the local host computer. Billing data could be accrued in real time, and the service company could disconnect or change the service of a customer at any time. Database updating is also simplified, and current information or changing data is always at hand (since it can be automatically included in a user database search). Moreover, the user can use just about any kind of computer to access the service company central facility. Furthermore, the connect time charges for communication networks are becoming more competitive in price, making this "direct connect" mode attractive for some applications.

The chief disadvantages of this "direct connect" approach are: Database access speed is much slower than in the locally-installed embodiment discussed above (because of the shared nature of the central facility and because of the relatively low data transmission rate of standard telephone lines); communications costs are much greater; and the service company must purchase and operate an expensive multi-user computer facility.

The "direct connect" and the locally stored database features might be used together in some applications. For example, the bulk of a database can be stored on and accessed locally from a local storage medium **100**. Database update file information can be stored and updated at a remote centralized facility and accessed via a telecommunications link to provide extremely current information in addition to the "older" information provided on-site.

There are thus both advantages and disadvantages to the "direct connect" mode. This mode may be offered as an option for users who require up-to-the-minute updated databases.

Once data is decrypted and stored into the memory of host computer **200** (e.g., for searching or manipulation rather than simply for display), it is susceptible to being intercepted by a "pirate" intercept program. System **10** bills for the data which is decrypted (so that the user would run up a huge bill if he tried to copy a large portion of a database). Nevertheless, it may be desirable in some applications to restrict the manner in which a customer can use decrypted data, while at the same time not restricting manipulations (e.g., browsing) of the decrypted data.

For example, keyword searching does not require a data image of the database (rather, it is most efficiently performed using index information **102**). However, other search techniques (e.g., final "zooming in" of the information being searched for) may require manipulation of a data image. It may be desirable to absolutely prevent the user from copying the decrypted data image information. However, the user should be able to manipulate data images in other ways (e.g., by browsing through full-text data and the like). It may be impossible to impose such restrictions on data stored in the user's own host computer **200** (or the user may be able to easily defeat such restrictions once imposed through skillful programming techniques).

FIG. **5** is a block diagram of an alternate embodiment of a database usage metering and protection system **500** in accordance with the present invention. The FIG. **5** embodiment includes a dedicated independent hardware unit ("browsing workstation") **501**, which can either act as a "stand-alone" or be designed to interface with additional data processing components.

Browsing workstation **501** in the preferred embodiment includes a proprietary, single-board computer **502** connected to a dedicated proprietary display station **504** having a secure environment. Computer **502** includes a bus connector **506**, a host interface **508**, a CPU **510**, a volatile, protected memory **512**, a non-volatile memory **513**, and a display driver **514**. Computer **502** is enclosed in a tamper-proof enclosure **516** to completely prevent access to its internal components except by authorized service personnel.

Computer **502** performs the decryption and billing functions discussed previously, and then stores the decrypted data into its own memory **512**. This arrangement allows the user to review ("browse") the information (on dedicated display station **504**) prior to sending desired information to his host computer (via interface **508** and connector **506**) for printing or other use. Thus, the decrypted database data image is first stored and manipulated by computer **502**. The user can be billed at one rate for browsing through or otherwise manipulating data in computer **502**, and billed at a higher rate for transferring data to his host computer (from which the data can be printed, stored, outputted, or telecommunicated to other computers and users).

02/28/2003, EAST Version: 1.03.0002

The user can evaluate the data while it is resident in computer memory **512** (via display station **504**) in order to decide whether or not he really wants the information transferred to his own host computer. In this way, very different billing rates can be provided for (a) browsing large amounts of full-text information and (b) actual use of information in the host computer (e.g., for word processing, telecommunications, printing, etc.).

Browsing workstation **501** may share some of the hardware and/or software of a host computer in order to reduce hardware costs—so long as information security is not significantly compromised. For example, one of the workstations normally connected to the host computer and its associated driver might be used in lieu of dedicated display station **504** and display driver **514** if there is little or no possibility that the user could copy a significant part of a database by reading information produced by the host computer display driver while browsing is in progress.

In a further embodiment, sophisticated software (not susceptible to manipulation or other misuse) could be temporarily loaded into the host computer (e.g., from storage medium **100**) and executed to provide the functionality of some or all of the hardware "blocks" shown in FIGS. **3** or **5**. Such software might use the security system provided by the host computer (and/or sophisticated techniques which are difficult to discover and "break") to create a protected environment within the host computer itself for decryption of database information and non-volatile storage of database usage information which may be adequately secure for various applications.

For example, although it may be undesirable to permit data type decryption key information to reside in the host computer permanently, the decryption key information can be temporarily provided by a protected memory device to the host computer. The host computer may then decrypt database information using the decryption key information, and destroy the key information after use. The host computer may decrypt database information "on the fly" and not retain much encrypted or decrypted information in memory at any one time to help prevent copying.

Although a dedicated hardware/software system typically provides the best assurance against tampering, techniques which may be implemented in software executing on a non-dedicated system may provide sufficient tamper resistance for some applications. For example, secure program control and usage information can be stored on a floppy disk which is accessed via the disk drive of a general-purpose non-dedicated personal computer. A non-volatile memory and logic device connected to the personal computer may (in conjunction with the secure program control software executing on the computer and/or a hardware controller connected to the computer) control and monitor the position of the read/write head of the disk drive, store the current head position in the non-volatile memory, and supervise execution of the secure program control software. Database usage information may be gathered by the program control software and stored on the floppy disk. Any attempts to tamper with the floppy disk which alters the last read/write head position may cause a warning message to be stored on the floppy disk in a database audit trail section of the disk (possibly along with cumulative messages indicating previous such occurrences) and may also result in destruction and/or disablement of the secure program control software.

While the present invention has been described with what is presently considered to be the most practical and preferred embodiments, it is to be understood that the appended claims are not to be limited to the disclosed embodiments, but on the contrary, are intended to cover modifications, variations, and/or equivalent arrangements which retain any of the novel features and advantages of this invention.

What is claimed is:

1. A secure database access system for use by at least one user, said system comprising:

an optical storage arrangement located at said user site, said storage arrangement storing at least one encrypted database component of at least one database, said database being adapted for being searched and retrieved in response to search criteria;

input means for providing database search criteria in response, at least in part, to user input;

searching means, operatively connected to said storage arrangement and to said input means, for searching and identifying a portion of said at least one database that corresponds to said search criteria;

reading means operatively connected to said searching means for reading an identified database portion so as to provide digital signals;

decrypting means, operatively connected to receive said provided digital signals, for decrypting an encrypted database portion; and

control means, operatively connected to at least one of (a) said storage arrangement, (b) said searching means, (c) said reading means, and (d) said decrypting means, for metering at least one of (a) processing, and (b) usage, of at least one part of said at least one database, and for facilitating communicating of information indicative of at least part of said metered at least one of (a) processing, and (b) usage, to at least one location distant from said user.

2. A secure database access system as in claim **1** wherein said control means includes a memory device storing information relating to said metering of at least one parameter of at least one of (a) processing, and (b) usage, said control means including means for inhibiting the decrypting of at least one portion of said at least one database portion in response to at least one budget setting a limit for use of at least one portion of said at least one database.

3. A secure database access system operable by at least one user at a user site, said system comprising:

an optical storage arrangement located at said at least one user site, said storage arrangement storing at least one database and at least one scrambled database component, said database being specially adapted for being searched and retrieved in response to search criteria;

input means for providing database search criteria in response, at least in part, to user input;

searching means, operatively connected to said storage arrangement and to said input means, for searching at least one part of said at least one database, including means for identifying portions of said at least one database in response to said search criteria;

reading means, operatively connected to said searching means, for reading an identified database portion so as to provide digital electrical signals;

descrambling means, operatively connected to receive provided digital electrical signals, for descrambling at least a portion of at least one scrambled database component so as to produce database information is useable form; and

control means operatively connected to at least one of (a) said storage arrangement, (b) said searching means, (c) said reading means, and (d) said decrypting means, for metering at least one of (a) processing, and (b) usage, of descrambled database components and for facilitating communication of information representing said metered at least one of (a) processing, and (b) usage, to at least one location distant from said user.

4. A secure database access system as in claim 1 or 3 wherein said control means communicates over a telephone network.

5. A system for permitting a client user to access and retrieve from stored digitally encoded database information of a type that is specially adapted for being searched and retrieved from in response to user-provided search criteria, said system also preventing unlimited user access to said stored database information so as to prevent said client user from at least one of (a) copying, (b) otherwise using, and (c) otherwise processing, said stored database information in a manner at least one of (a) not authorized by the publisher of said database information, and (b) so as to ensure that the publisher of said database information is adequately compensated for at least one of (i) client user access, and (ii) client user use, said system including in combination:

at least one housing located at said client site;

at least one portable storage medium adapted to be accepted by said housing, said at least one storage medium storing, at least in part, at least one database having at least a part that is encrypted and stored in a form making said part unintelligible to said client user unless said part is decrypted, said database being at least in part indexed by at least one index;

digital processor means operatively connected to said at least one storage medium so as to (a) generate a database access request, (b) read index information from said at least one storage medium so as to provide corresponding digital index signals, (c) identify, at least partially in response to said digital index signals, portions of said at least one database which satisfy the access request, and (d) read an identified database portion from the at least one storage medium so as to provide corresponding digital signals for at least one of (a) processing, and (b) usage; and

control means operatively connected to at least one of (a) said digital processor means, and (b) said at least one storage medium, for metering at least one aspect of at least one of (a) processing, and (b) usage, of said at least one database, for storing digital signals indicative of at least one part of said metered at least one aspect in a form not easily modified by said client user, and for selectively limiting, in response to said at least one of metered (a) processing, and (b) usage, the further at least one of (a) processing, and (b) usage, of at least a part of said at least one database.

6. A system as in claim 5 wherein said at least one storage medium includes an optical storage component.

7. A secure database access system for permitting a user to access, retrieve from, and use stored digitally encoded database information, said system comprising:

at least one housing;

at least one storage medium located at said user site and adapted to be insertable into and physically removable from said housing by said user, said at least one storage medium comprising an optical storage medium, said at least one storage medium storing digitally encoded database information that is, at least in part, encrypted;

input means for providing database search criteria at least in part specified by said user;

searching means, operatively connected to said at least one storage medium and to said input means, for identifying a portion of said database information corresponding to said search criteria, said searching means also including reading means for reading at least one digital signal corresponding to at least part of said identified database from said at least one storage medium;

means for decrypting said digital signals so as to produce corresponding, decrypted database information; and

control means, connected to said searching means, for metering at least part of at least one of (a) processing, and (b) usage, of database information, and for preventing at least one of (a) processing, and (b) using, of at least a part of said at least one database in response to at least one of (a) said metered processing, and (b) said metered usage.

8. A system as in claim 7 wherein said user is located at a physical site and said at least one storage medium is located at the same physical site as said user.

9. A secure database access system for permitting a client user to access and retrieve from digitally encoded database contents stored in a form at least in part specially adapted for being searched, said system also preventing unlimited user access to said stored database contents so as to prevent said user from at least one of (a) copying, (b) otherwise using, and (c) otherwise processing, said stored database contents in a manner at least one of (a) not authorized by the publisher of said database, and (b) so as to ensure that the publisher of said database is adequately compensated for at least one of (i) user access, and (ii) user use, said system comprising:

at least one housing;

at least one storage medium adapted to be accepted by said housing and storing at least part of at least one database, said at least one database having at least one encrypted component, said at least one database also comprising a digital collection of information, said digital collection of information having been processed at least in part so as to be searchable;

at least one processor, operatively connected to said at least one storage medium, said at least one processor preprogrammed so as to: (a) accept search criteria at least in part specified by a user, (b) search at least one part of said at least one database in response to said search criteria, (c) identify, in accordance with said search, any portions of said at least one database which satisfy said search criteria, (d) read information from said at least one storage

medium, and (e) provide signals corresponding at least in part to an identified database portion;

decrypting means for decrypting signals provided by said processor so as to provide corresponding database contents in useable form; and

control means, coupled to at least one of (a) said at least one processor, and (b) said decrypting means, for measuring the percentage of at least one part of said information collection decrypted by said decrypting means, for storing said measured percentage in a form not readily modifiable by said client user, and for preventing at least one part of said at least one information collection from being provided in useable form.

10. A method of securing access to at least one database comprising the steps of:

providing at least one portable medium located at a client site and storing at least one database composed, at least in part, of information organized as digital indicia in database searchable form, said at least one database having at least one encrypted part in order to preclude at least one of (a) unauthorized use, and (b) unauthorized access;

generating database search criteria;

searching at least one part of said at least one database to identify digital indicia corresponding to portions of said at least one database which satisfy said generated search criteria;

decrypting at least one of (a) digital electronic signals corresponding to desired, identified, encrypted database portions, and (b) at least one digital electronic signal corresponding to an identified encrypted portion of said at least one database, to produce corresponding decrypted information;

measuring at least one of (a) the quantity, and (b) the duration, of use of at least one portion of said at least one database and generating a result corresponding to said measurement;

storing an indication of said generated result on a storage medium in a form which deters client tampering therewith; and

selectively inhibiting at least one of (a) searching, (b) decrypting, and (c) otherwise using, in response to said result.

11. A database access system comprising:

a storage arrangement storing at least one database at a customer site, said at least one database having at least one encrypted part, and also storing information representing at least one database usage ceiling corresponding to at least one portion of said at least one database;

updating means, operatively connected to said storage arrangement for updating at least one part of said stored database usage ceiling information;

input means, operatively connected to said storage arrangement, for generating database search criteria at least in part in response to user input;

searching means, operatively connected to said storage arrangement and operatively connected to receive said generated search criteria, for searching at least one part of said at least one database and for identifying any portions of said at least one part of said at least one database which correspond to said search criteria;

retrieving means for retrieving an identified portion of said database from said storage arrangement;

decrypting means operatively connected to said retrieving means for decrypting a retrieved database portion; and

control means operatively connected to at least said storage arrangement, for metering at least one parameter of usage of at least one portion of said at least one database, for comparing said metered usage to said at least one database usage ceiling, and for selectively preventing decrypting of at least one part of said encrypted database in response to the result of said comparison.

12. A secure database access system for permitting at least one client user to access, and retrieve from, digitally encoded database contents stored in a form at least in part adapted for being searched, said system also preventing unlimited user access to said stored database contents so as to prevent said at least one client user from copying or otherwise using or processing said stored database contents in a manner at least one of (a) not authorized by the publisher of said database, and (b) so as to ensure that the publisher of said database is adequately compensated for at least one of (i) user access, and (ii) user use, said database access system comprising:

at least one database having at least one part in unusable form;

at least one housing;

at least one optical storage means located at the same physical site as said at least one client user and adapted to be accepted by said housing, said optical storage means for storing at least part of said at least one database;

input means for providing database search criteria at least in part determined by client user input;

searching means, operatively connected to said input means, for searching at least one part of said at least one database to identify database portions and for producing corresponding digital signals;

transforming means, operatively connected to receive said corresponding digital signals, for transforming at least one digital signal representing at least one of (i) at least one database section, and (ii) any user desired database sections, from unusable form into useable form through the use of a key;

metering means, operatively connected to at least one of (a) said searching means, (b) said transforming means, and (c) said at least one optical storage means, for metering at least one parameter indicative of at least one of (a) usage, and (b) processing, of database contents so as to produce a metered result; and

preventing means, operatively connected to said metering means, for selectively preventing at least one of (a) transforming of database portions into useable form, and (b) use of useable form database portions, in response to said metered result.

13. A method of providing database information in a secure manner, said method comprising:

providing at a client user site at least one portable storage medium storing at least a portion of a database having at least one encrypted part;

inputting database search criteria determined at least in part by user input;

searching at least one part of said database, identifying at least a portion of said database in response to said search, and providing digital signals corresponding to said identified at least a portion;

decrypting said provided digital signals so as to at least one of (a) automatically decrypt at least one of said identified database portions, and (b) at least in part decrypt at least one of said identified database portions;

monitoring at least one of (a) said searching step, (b) said selecting step, and (c) said decrypting step, so that at least one parameter indicative of the usage of database portions is metered and stored in a tamper resistant form; and

preventing decrypting of at least a part of an encrypted database portion of said at least one database in response to said metered parameter.

14. A database access system which is capable of being operated by a user at a user site so as to electronically search digital database information in response to a search request, said system including the following combination of elements all located at said user site;

an optical storage device storing thereon digitally encoded database information at least some of which is in a form that is unintelligible unless said information is processed using a key;

a search/retrieval arrangement operatively coupled to said optical storage device, said search/retrieval arrangement causing a subset of said database information responsive, at least in part, to said search request to be retrieved from said storage device, processed using said key, and presented to said user; and

a metering arrangement operatively associated with said optical storage device, said metering arrangement monitoring usage of said database information, storing information indicative of at least a portion of said usage, and selectively inhibiting said database information from being processed to said user in response to comparison of monitored usage with a predetermined limit.

15. A method for permitting user access to, and retrieval from, stored digitally encoded database contents, said database contents being adapted for searching and retrieving, said method comprising the steps of:

(a) storing database information on an optical storage device physically located at a client site in an encrypted form that is unintelligible to said user unless said information is processed using at least one key;

(b) selecting at least one portion of said stored database information based on selection criteria determined at least in part by user input and providing digital electrical signals corresponding to selected information;

(c) decrypting said provided digital electrical signals through the use of said at least one key so as to permit use of at least a part of said selected database portion;

(d) metering information representing at least part of at least one of (a) use, and (b) processing, of said database portion processed by said step (c);

(e) storing said representative information in a manner inaccessible to the typical user; and

(f) selectively preventing decryption of at least one encrypted part of said database in response to said metered information.

16. A method for permitting user access to, and retrieval from, stored digitally encoded database contents, said database contents being adapted for searching and retrieving, said method comprising the steps of:

(a) storing database information on an optical storage device physically located at a client site in an encrypted form unintelligible to said user unless processed using at least one digital signal key;

(b) selecting at least one portion of said stored database information based on selection criteria determined at least in part by user input and providing digital signals corresponding to selected information;

(c) decrypting said provided digital signals through the use of at least one digital signal key so as to permit use of at least a part of said selected database portion;

(d) metering information representing at least part of at least one of (a) use, and (b) processing, of a database portion so as to provide digital signals; and

(e) conveying information reflecting at least some of said provided digital signals to at least one location distant from said client site.

17. A method of providing information responsive to search criteria for use by a client at a physical client site, said method comprising the steps of:

(1) providing, for insertion into a reading device at said physical client site, at least one portable optical storage medium, said optical storage medium storing database information adapted to be searchable;

(2) inserting said optical storage medium into said reading device;

(3) searching said database information to identify database information which corresponds, at least in part, to said search criteria;

(4) reading and processing identified database information from said optical storage medium using a key; and

(5) metering at least one aspect of client usage of said database information and generating at least one parameter reflecting said usage.

18. A method of securing access to at least one database comprising the steps of:

providing at least one storage medium located at a client site and storing at least one database having at least one encrypted database part, at least part of the contents of said at least one database having been preprocessed so as to be searchable;

providing database search criteria determined at least partly by user input;

searching at least one part of the at least one database for at least one portion of said at least one database corresponding to said search criteria;

decrypting at least one of (a) at least one digital electronic signal corresponding to an encrypted database portion resulting from said searching, and (b) digital electronic signals which correspond to any user desired ones of any encrypted, database portions resulting from said searching, and producing corresponding decrypted information therefrom; and

restricting use of at least a part of said produced decrypted information by preventing, under at least one circumstance, performance of at least one of copying, storing, printing, and communicating with respect to said useable information.

19. A method of securing access to a database comprising the steps of:

providing at a client site at least one mass storage medium including optical memory means, said storage medium storing at least one searchable

database, said database having at least some inaccessible contents;

providing database search criteria determined at least in part by user input;

searching at least one part of said at least one database in response to said database search criteria and locating any database portions which corresponds to said search criteria;

making accessible at least one of (a) at least one portions of the inaccessible database contents resulting from said searching, and (b) any user desired ones of inaccessible database contents resulting from said searching, so as to provide corresponding useable information, including the step of processing said contents through the use of a key; and

selectively restricting use of at least one portion of said at least one database by preventing, under at least one circumstance, at least one of copying, storing, printing and communicating.

20. A secure database access system comprising:

at least one storage medium located at a customer site and storing database information on at least one removable, optical storage disc, with at least one part of said database information being stored encrypted form;

input means for providing database search criteria in response, at least in part, to user input;

searching means, operatively connected to said at least one storage medium and to said input means, for searching at least one portion of said database information so as to identify database portions corresponding to said search criteria;

additional functions means, operatively connected to said searching means, for performing at least one of the additional functions of copying, storing, printing, and communicating at least one part of said identified database information;

decrypting means, operatively connected to at least one of (a) said searching means, and (b) said at least one storage medium, for decrypting identified database information;

displaying means, operatively connected to at least one of (a) said searching means, and (b) said decrypting means, for displaying database information; and

selectively restricting means, operatively connected to said additional function means, for restricting the use of at least one database portion by permitting said displaying means to display, but precluding said additional functions means from at least one of copying, storing, printing and communicating, at least one part of identified database information.

21. A secure database access system of the type for electronically searching digital database information in response to a user search request, said system including a data processor arrangement coupled to writable volatile storage, writable non-volatile storage, a user input device, and a display, said system further including:

at least one optical disk having encrypted digitally encoded database information stored thereon;

an optical disk drive directly connected to and local with said data processor arrangement and adapted to physically accept and interact with said optical disk, said optical disk drive reading stored database information from said optical disk and providing corresponding signals to said data processor arrangement;

said data processor arrangement being connected to receive said signals generated by said optical disk drive, said data processor arrangement being preprogrammed so as to perform the following functions:

(a) cooperate with said optical disk drive so as to search said digitally encoded database information, at least in part, in response to a user search request inputted via said user input device and to retrieve signals representing at least some of said stored digitally encoded database information in response to said search,

(b) decrypt at least some of said retrieved signals so as to provide corresponding decrypted signals,

(c) display information responsive to at least some of said retrieved signals,

(d) update at least one indication related to at least one of (a) processing, and (b) usage, of database information,

(e) selectively permit, at least in part in response to said updated indication, information corresponding to at least some of said decrypted signals to be recorded on a non-volatile medium.

22. A method of securing the distributing of properties, said method comprising the steps of:

installing at a client user site at least one portable storage medium having plural properties stored thereon in digital form, rights in said plural properties being owned by plural property owners, including the steps of providing at least one portion of said plural properties in encrypted form and the step of requiring at least one decryption key for transforming encrypted portions of said plural properties into a form allowing at least one of (a) their using, and (b) their accessing;

selectively preventing the usage of at least one of (a) a percentage of any of said plural properties, (b) a subset of at least one portion of at least one plural property, (c) a percentage of all said plural properties, and (d) at least one of said plural properties;

generating, at said client site, digital electronic signals for at least one aspect of client usage of said properties by at least one client;

requiring said client to pay a payment; and

apportioning at least a portion of client payments between plural property owners.

23. A method as in claim 22 wherein said method further includes communicating said generated information to at least one location remote to said client site.

24. A secure digital access system for distributing properties in digital form, said system comprising:

first storage means physically disposed at a client site and including an optical storage device, said storage means for storing plural properties thereon in digital from, rights in said properties being owned by plural property owners, the contents of at least a part of at least one of said plural properties being secured by at least one of (a) encryption, and (b) a password;

digital processor means, operatively connected to said first storage means, for allowing at least one client user to select and electronically retrieve at least one part of at least one of said stored properties, said digital processor means also including means for allowing said client user to at least one of (a) access and (b) use, at least one secured part of said plural properties through use of at least one key;

usage means, operatively connected to at least one of (a) said digital processor means, and (b) said first storage means, for providing digital usage information representing at least one aspect of user usage of properties;

communicating means, operatively connected to at least one of (a) said further storage means, and (b) said digital processor means, for facilitating communication of indicia of said usage information to at least one location distant from said client site;

determining means, operatively connected to said communicating means, for determining any client payments due;

requiring means, operatively connected to at least one of (a) said digital processor means, (b) said determining means, (c) said communicating means, and (d) said usage means, for requiring payment from said client; and

means, operatively connected to receive at least part of said digital usage information, to at least in part apportion amongst plural property owners at least a portion of said user payment, at least in part, at least one of (a) in response to said digital usage information, and (b) according to respective ownership rights of said plural property owners.

25. A method of distributing properties in digital form comprising:

providing at least one optical storage means at a client site having plural properties stored thereon in digital form, rights in said properties being owned by plural property owners, at least part of at least one of said plural properties being encrypted;

searching and electronically retrieving from at least one part of said stored plural properties;

using at least one portion of a retrieved part of said plural properties;

determining a payment due from said client;

apportioning at least a portion of said client payment between plural property owners; and

controlling user access to said plural properties.

* * * * *